



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,948	12/22/1999	HIROYUKI KURUMATANI	500.38035X00	4306

7590 12/23/2003

ANTONELLI TERRY STOUT & KRAUS  
1300 NORTH SEVENTEENTH STREET  
SUITE 1800  
ARLINGTON, VA 22209

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 12/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/468,948

Applicant(s)

KURUMATANI, HIROYUKI

Examiner

Douglas J. Meislahn

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 December 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. §§ 119 and 120

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_ 6) ☐ Other: \_\_\_\_

## **DETAILED ACTION**

### ***Drawings***

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: 201, 401, 413, 501, 509, 601, 711, 712, 801, 813, 903, 907, 909, 911, 912, 914, 1101, 1201, 1211, 1301, 1401, 1409, and 1609. A proposed drawing correction, corrected drawings, or amendment to the specification to add the reference sign(s) in the description, are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance. In line 26 on page 44, "1011" should be "1211". In line 13 of page 52, "1608" should be "1609".
2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "914" has been used to designate two elements, neither of which are referred to by number in the specification. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

### ***Claim Objections***

3. Claims 7 and 12 are objected to because of the following informalities: in the first clauses of the claims, "an" should either be "a", "the", or, most preferably, deleted. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-5 and 7-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. Claims 1, 7, and 12 recite the limitations "said inputted coordinate component x1" in their second clauses, "said coordinate component x2" in the fourth clauses, "said projective coordinate  $[X_2, Z_2]$ " in the fifth clauses, "said coordinate component x4" in the sixth clauses, "said projective coordinate  $[X_4, Z_4]$ " in the seventh clauses, "said stored projective coordinates  $[X_1, Z_1]$ ,  $[X_2, Z_2]$  and  $[X_4, Z_4]$ " in the eighth clauses, and "said coordinate component x3" in the ninth clauses. There is insufficient antecedent basis for these limitations in the claims. In all cases, deleting "said" would overcome the rejection. The offending recitations of "said" could also be replaced with "the".

7. Claims 2, 3, 8, and 9 recite the limitations "the x-coordinates" in the fourth clauses and "said stored random number  $k$ " in the last clauses. There is insufficient antecedent basis for these limitations in the claims. The claims are entirely unclear as to which x-coordinates are transformed. This ambiguity makes impossible a precise comparison of the claims with the prior art. Change "said" to "the".

8. Claims 4 and 10 recite the limitations "said computed B" in their second clauses, "said determined  $Z_3$ " in their fifth clauses, and "said stored  $Z_3$ " in their sixth clauses. There is insufficient antecedent basis for this limitation in the claim. Change the recitations of "said" to "the".

9. Claims 5 and 11 recite the limitation "said computed B" in their second clauses. There is insufficient antecedent basis for this limitation in the claim. Change "said" to "the".

***Claim Rejections - 35 USC § 101***

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-5 and 7-12 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The subject matter of the claims is mathematical manipulations that are not put to an useful purpose. Including a step in which a the mathematical manipulations are used in a cryptographic operation would make the claims statutory. To emphasize the distinction, encrypting data is an useful process and hence statutory; adding numbers, even if the are points on an elliptic curve, is not necessarily beneficial and hence is non-statutory.

***Double Patenting***

11. Claim 12 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 7. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

***Claim Rejections - 35 USC § 102***

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1, 4-7, and 10-12 are rejected under 35 U.S.C. 102(a) as being clearly anticipated by Vanstone et al. (EP 0 874 307 A1). See pages 5-8.

14. Claims 1, 6, 7, and 12 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Agnew et al. ("An Implementation of Elliptic Curve Cryptosystems Over F2155"). See pages 804-813.

***Claim Rejections - 35 USC § 103***

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 2, 3, 8, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. in view of Chudnovsky et al. ("Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests").

Vanstone et al. present a system of improving the speed of elliptic curve cryptography. They do not say that a random number is used to derive projective coordinates according to the equations given in the claims. Chudnovsky et al. present methods for improving the speed of elliptic curves. As detailed above, the scope of

these claims is indefinite, but the examiner believes that, were the scope of the claims clearly defined, the teachings of these two references would render the claims obvious.


***Conclusion***

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Miyaji et al. (5442707), Miyaji (5497423), and Crandall et al. (6307935).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

  
Douglas J. Meislahn  
Examiner  
Art Unit 2132

DJM